

# Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

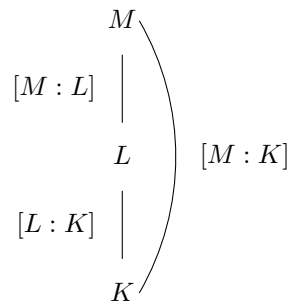
Mohamed NASSIRI

## INTRO

Une extension de corps est la donnée d'un morphisme injectif de corps  $i : K \rightarrow L$ , où  $K$  et  $L$  sont des corps. On la note  $K \subset L$ . Ainsi, si  $K$  est un sous-corps de  $L$ , alors  $L$  est un  $K$ -espace vectoriel. Dans le cadre où  $\dim_K L$  est finie, on définit le *degré de l'extension  $L$  sur  $K$*  par  $[L : K] = \dim_K L$ . A partir de là, vient le *théorème de la base télescopique*, et son corollaire dit de la *multiplicativité des degrés* : Soit  $K \subset L \subset M$  des corps, si les degrés sont finis, on a

$$[M : K] = [M : L][L : K]$$

On représente souvent les extensions de corps comme le schéma ci-dessous en indiquant accessoirement les degrés des extensions.



## Références

- [GRI] Algèbre linéaire 5e Edition, Joseph Grifone
- [GOUag] Les maths en tête : Algèbre, Xavier Gourdon
- [GOZ] Théorie de Galois, Ivan Gozard ♠
- [PER] Cours d'Algèbre, Daniel Perrin ♠
- [ROU] Petit guide de calcul différentiel, François Rouvière ♠

## Développements

De la dualité dans  $\mathcal{M}_n(\mathbb{R})$   
Théorème de Wedderburn

Dans toute la leçon, sauf mention contraire,  $K$  est un corps commutatif et  $E \neq \{0\}$  un  $K$ -e.v.

(ii) On dit que l'espace  $E$  est de dimension finie s'il admet une famille génératrice finie.

(iii) Une famille de vecteurs  $(v_1, \dots, v_p)$  d'un e.v.  $E$  est dite libre si :

$$\lambda_1 v_1 + \dots + \lambda_p v_p = 0 \Rightarrow v_1 = \dots = v_p = 0$$

(iv) On appelle base une famille à la fois libre et génératrice.

## 1 Dimension d'un espace vectoriel [GRI] p.10 → 28

### 1.1 Familles libres, familles génératrices

**Définition 1** (i) Une famille de vecteurs  $(v_1, \dots, v_p)$  d'un e.v.  $E$  est dite génératrice si  $E = \text{vect}\{v_1, \dots, v_p\}$ .

**Proposition 2** (i) Une famille  $(v_1, \dots, v_p)$  est une base de  $E$  si et seulement si tout  $x \in E$  se décompose d'une façon unique sur les  $v_i$ .

(ii) Soit  $\mathcal{B} = (v_1, \dots, v_n)$  une base de  $E$ . Alors il

existe une bijection

$$E \rightarrow K^n$$

$$x = x_1 v_1 + \dots + x_n v_n \mapsto (x_1, \dots, x_n)$$

Les scalaires  $x_i$  sont dits composantes de  $x$  dans la base  $\mathcal{B} = (v_1, \dots, v_n)$

**Exemple 3** (i) La famille

$$\underbrace{((1, 0, 0, \dots, 0))}_{=e_1}, \underbrace{(0, 1, 0, \dots, 0)}_{=e_2}, \dots, \underbrace{(0, 0, 0, \dots, 1)}_{=e_n}$$

est une base de  $K^n$ , dite base canonique.

(ii) La famille  $(1, X, X^2, \dots, X^n)$  est une base de  $\mathbb{R}_n[X]$  (e.v. polynômes de degré inférieur ou égal à  $n$ ).

**Théorème 4** (i) De toute famille génératrice on peut extraire une base.

(ii) Théorème de la base incomplète Toute famille libre peut être complétée de manière à former une base.

## 1.2 Théorèmes fondamentaux sur la dimension

**Théorème 5** Dans un  $K$ -e.v.  $E$  de dimension finie, toutes les bases ont le même nombre d'éléments. Ce nombre est appelé dimension de  $E$  sur  $K$  et est noté  $\dim_K(E)$  (ou  $\dim(E)$  s'il n'y a pas d'ambiguïté).

**Corollaire 6** Dans un e.v. de dimension  $n$ , toute famille ayant plus de  $n$  éléments est liée.

Dans un e.v. de dimension  $n$ , les familles ayant moins de  $n$  éléments ne peuvent être génératrices.

**Proposition 7** Soient  $E_1, \dots, E_p$  des e.v. de dimension finie sur le même corps  $K$ . Alors :

$$\dim_K(E_1 \times \dots \times E_p) = \dim_K(E_1) + \dots + \dim_K(E_p)$$

**Théorème 8** Soit  $E$  un e.v. de dimension  $n$ . Alors :

(i) Toute famille génératrice ayant  $n$  éléments est une base.

(ii) Toute famille libre ayant  $n$  éléments est une base.

**Proposition 9** Soit  $E$  un e.v. de dimension  $n$  et  $F$  un s.e.v. de  $E$ . Alors  $F$  est de dimension finie, et de plus :

$$(i) \dim_K(F) \leq \dim_K(E).$$

$$(ii) \dim_K(F) = \dim_K(E) \Leftrightarrow F = E.$$

## 1.3 Somme, somme directe, sous-espaces supplémentaires

**Définition 10** Soient  $E_1, E_2$  deux s.e.v. d'un e.v.  $E$ . On appelle somme de  $E_1$  et  $E_2$  le sous-espace de  $E$  défini par :

$$E_1 + E_2 = \{x \in E ; \exists (x_1, x_2) \in E_1 \times E_2, x = x_1 + x_2\}$$

**Proposition-Définition 11** Soient  $E_1, E_2$  deux s.e.v. d'un e.v.  $E$ , et soit  $\mathcal{E} = E_1 + E_2$ .

La décomposition de tout élément de  $\mathcal{E}$  en somme d'un élément de  $E_1$  et d'un élément de  $E_2$  est unique si et seulement si  $E_1 \cap E_2 = \{0\}$ . On écrit alors :

$$\mathcal{E} = E_1 \oplus E_2$$

On dit alors que  $\mathcal{E}$  est somme directe de  $E_1$  et  $E_2$ .

**Proposition 12** Soient  $E_1, E_2$  deux s.e.v. d'un e.v.  $E$ . Alors  $E = E_1 \oplus E_2$  si et seulement si pour toute base  $\mathcal{B}_1$  de  $E_1$  et toute base  $\mathcal{B}_2$  de  $E_2$ ,  $(\mathcal{B}_1, \mathcal{B}_2)$  est une base de  $E$ .

**Définition 13** Soient  $E_1, E_2$  deux s.e.v. d'un e.v.  $E$ . On dit que  $E_1$  et  $E_2$  sont supplémentaires (ou que  $E_2$  est un supplémentaire de  $E_1$ ) si  $E = E_1 \oplus E_2$ .

**Corollaire 14** Soit  $E$  un e.v. de dimension finie. Pour tout s.e.v.  $E_1$  de  $E$ , il existe toujours un supplémentaire.

Le supplémentaire de  $E_1$  n'est pas unique mais tous les supplémentaires de  $E_1$  ont même dimension.

**Théorème 15** Soit  $E$  un e.v. de dimension finie. Alors

$$E = E_1 \oplus E_2 \Leftrightarrow \begin{cases} E_1 \cap E_2 = \{0\} \\ \dim(E) = \dim(E_1) + \dim(E_2) \end{cases}$$

**Proposition 16** Soient  $E_1, E_2$  deux s.e.v. d'un e.v.  $E$ . Alors

$$\dim(E_1 + E_2) = \dim(E_1) + \dim(E_2) - \dim(E_1 \cap E_2)$$

En particulier,

$$\dim(E_1 \oplus E_2) = \dim(E_1) + \dim(E_2)$$

**Théorème 17** On peut généraliser les résultats avec  $E_1, \dots, E_p$  s.e.v. d'un e.v.  $E$ .

On a alors

$$(i) \dim(E_1 \oplus \dots \oplus E_p) = \dim(E_1) + \dots + \dim(E_p)$$

(ii)  $E = E_1 \oplus \dots \oplus E_p$  si et seulement si :

$$- E = E_1 + \dots + E_p$$

$$- \dim(E) = \dim(E_1) + \dots + \dim(E_p)$$

(iii)  $E = E_1 \oplus \dots \oplus E_p$  si et seulement si :

$$- E_1 \cap E_2 = \{0\}$$

$$- (E_1 + E_2) \cap E_3 = \{0\}$$

$$- (E_1 + E_2 + E_3) \cap E_4 = \{0\}$$

...

$$- (E_1 + E_2 + \dots + E_{p-1}) \cap E_p = \{0\}$$

## 2 Applications linéaires

### 2.1 Applications linéaires et rang [GRI] p.59 → 63

**Proposition-Définition 18** Soient  $E, E'$  deux e.v. de dimension finie et  $f : E \rightarrow E'$  une application linéaire.

Soit  $F$  un s.e.v. de  $E$ . Alors  $f(F)$  est un s.e.v. de  $E'$ .

En particulier,  $f(E)$  est un s.e.v. de  $E'$  appelé image de  $f$  et noté  $\text{Im}(f)$ . Sa dimension est appelé rang de  $f$  et est noté  $\text{rg}(f)$ .

**Proposition-Définition 19** Soit  $f \in \mathcal{L}(E, E')$ . Alors

(i)

$$\text{Ker}(f) = \{x \in E \mid f(x) = 0\}$$

est un s.e.v. de  $E$  appelé noyau de  $f$ .

(ii)  $f$  est injective si et seulement si  $\text{Ker}(f) = \{0\}$ .

**Proposition 20** Soient  $f \in \mathcal{L}(E, E')$  et  $(v_i)_{i \in I}$  une famille de vecteurs de  $E$ .

(i) Si  $f$  est injective et la famille  $(v_i)_{i \in I}$  est libre, alors la famille  $(f(v_i))_{i \in I}$  est libre.

(ii) Si  $f$  est surjective et la famille  $(v_i)_{i \in I}$  est génératrice, alors la famille  $(f(v_i))_{i \in I}$  est génératrice.

En particulier, si  $f$  est bijective et la famille  $(v_i)_{i \in I}$  est une base, alors la famille  $(f(v_i))_{i \in I}$  est une base.

**Proposition 21** Deux espaces vectoriels de dimension finie sont isomorphes si et seulement s'ils ont même dimension.

**Théorème 22** Théorème du rang

Soit  $f \in \mathcal{L}(E, E')$ . Alors

$$\dim(E) = \text{rg}(f) + \dim(\text{Ker}(f))$$

**Corollaire 23** Soient  $E, E'$  deux e.v. de même dimension finie et  $f \in \mathcal{L}(E, E')$ . Alors les assertions suivantes sont équivalentes :

(i)  $f$  est injective.

(ii)  $f$  est surjective

(iii)  $f$  est bijective

**Remarque 24** Ce résultat est faux en dimension infinie comme le montre le contre-exemple suivant : l'application

$$\begin{aligned} D : \mathbb{R}[X] &\rightarrow \mathbb{R}[X] \\ P &\mapsto P' \end{aligned}$$

est surjective et non injective.

### 2.2 Matrices et applications linéaires [GRI] p.66, p80-81

**Proposition 25** Soient  $E, E'$  deux e.v. de dimension  $n$  et  $p$  respectivement,  $(e_i)$  et  $(\epsilon_j)$  des bases de

$E$  et  $E'$  respectivement et enfin  $f \in \mathcal{L}(E, E')$ .

Alors l'application

$$\begin{aligned} \mathcal{L}(E, E') &\rightarrow \mathcal{M}_{p,n}(K) \\ f &\mapsto M(f)_{e_i, \epsilon_j} \end{aligned}$$

**Définition 26** (i) Soit  $(v_i)_{i \in I}$  une famille de vecteurs. On appelle rang de la famille la dimension de l'espace engendré par les vecteurs  $(v_i)_{i \in I}$ .

(ii) Soit  $A = \|\|c_1, \dots, c_n\| \in \mathcal{M}_{p,n}(K)$ . On appelle rang de la matrice  $A$  le rang de la famille des vecteurs colonnes de  $A$  :

$$\text{rg}(A) = \text{rg}((c_1, \dots, c_n)) = \dim(\text{vect}\{v_1, \dots, v_p\})$$

**Proposition 27** Soient  $E, F$  deux e.v. de dimension  $n$  et  $p$  respectivement,  $(e_i)$  et  $(\epsilon_j)$  des bases de  $E$  et  $F$  respectivement et enfin  $f \in \mathcal{L}(E, F)$ , et  $A = M(f)_{e_i, \epsilon_j}$ . Alors

$$\text{rg}(f) = \text{rg}(A)$$

**Remarque 28** On aura besoin, dans le cadre de la dualité, du résultat suivant (qu'on ne démontre pas) : pour toute matrice  $A$ , on a  $\text{rg}(A) = \text{rg}({}^t A)$

## 3 Dualité

### 3.1 Formes linéaires, espace dual et hyperplans

**Définition 29** On appelle forme linéaire sur  $E$  une application linéaire  $\varphi : E \rightarrow K$ .

L'ensemble des formes linéaires  $\mathcal{L}_K(E, K)$  est noté  $E^*$  est dit espace dual de  $E$ . [GOUag] p.126

**Exemple 30** •  $\text{Tr} : \mathcal{M}_n(\mathbb{R}) \rightarrow \mathbb{R}, A \mapsto \text{Tr}A$

•  $C([0, 1], \mathbb{R}) \rightarrow \mathbb{R}, f \mapsto \int_0^1 f(t) dt$ . [GOUag] p.126

**Proposition-Définition 31** Soit  $E$  de dimension finie  $n$ , et  $\varphi \in E^*, \varphi \neq 0$ . On a :

$$\dim(\text{Ker}\varphi) = n - 1$$

$\text{Ker}\varphi$  est dit hyperplan de  $E$  déterminée par  $\varphi$ . [GRI] p.82

**Exemple 32** •  $\{A \in \mathcal{M}_n(\mathbb{R}) \mid \text{Tr}A = 0\}$  est un hyperplan.

•  $\{(x, y, z) \in \mathbb{R}^3 \mid 3x + 2y + z = 0\}$  est un hyperplan. [GRI] p.82

### 3.2 Etude du dual et du bidual [GOUag] p.127

**Définition 33** Soit  $B = (e_1, \dots, e_n)$  une base de  $E$ . Pour tout  $i, 1 \leq i \leq n$ , la forme linéaire  $e_i^*$  définie sur  $B$  par  $e_i^*(e_j) = 0$  si  $i \neq j$ ,  $e_i^*(e_i) = 1$ , s'appelle forme linéaire coordonnée d'indice  $i$ .

**Théorème 34** Soit  $B = (e_1, \dots, e_n)$  une base de  $E$ . Alors  $B^* = (e_1^*, \dots, e_n^*)$  est une base de  $E^*$  appelée base duale de  $B$ , et donc  $\dim E^* = \dim E$ . Pour tout  $\varphi \in E^*$ , on a  $\varphi = \sum_{i=1}^n \varphi(e_i) e_i^*$ .

**Application 35** Soit  $E$  un  $\mathbb{K}$ -e.v,  $\varphi_1, \dots, \varphi_p \in E^*$  et  $\varphi : E \rightarrow \mathbb{K}^p$  définie par  $\varphi = (\varphi_1, \dots, \varphi_p)$ . Alors  $\varphi$  est surjectif si et seulement si  $\varphi_1, \dots, \varphi_p$  sont linéairement indépendants.

### Théorème 36 ♠ De la dualité dans $\mathcal{M}_n(\mathbb{R})$ ♠

• Soit  $A \in \mathcal{M}_n(\mathbb{K})$ . L'application

$$f_A : \mathcal{M}_n(\mathbb{K}) \rightarrow \mathbb{K} \\ X \mapsto \text{Tr}(AX)$$

induit un isomorphisme entre  $\mathcal{M}_n(\mathbb{K})$  et  $(\mathcal{M}_n(\mathbb{K}))^*$

• Soit  $f : \mathcal{M}_n(\mathbb{K}) \rightarrow \mathbb{K}$  une forme linéaire telle que  $f(XY) = f(YX)$ ,  $\forall X, Y \in \mathcal{M}_n(\mathbb{K})$ . Alors  $\exists \lambda \in \mathbb{K}$  tel que  $f(X) = \lambda \text{Tr}(X)$ .

•  $\forall n \geq 2$ , tout hyperplan de  $\mathcal{M}_n(\mathbb{K})$  rencontre  $\text{GL}_n(\mathbb{K})$ . [FGNag1] p.329 → 331

**Théorème 37** Si  $x \in E$ , on note  $\tilde{x} : E^* \rightarrow \mathbb{K}$ ,  $\varphi \mapsto \varphi(x)$ . On a  $\tilde{x} \in E^{**}$  et l'application  $f : E \rightarrow E^{**}$ ,  $x \mapsto \tilde{x}$  est un isomorphisme.

**Proposition 38** Soit  $(f_1, \dots, f_n)$  une base de  $E^*$ . Il existe une unique base  $(e_1, \dots, e_n)$  de  $E$  telle que pour tout  $i$ ,  $e_i^* = f_i$ .

**Définition 39** Cette base s'appelle base antéduale de  $(f_1, \dots, f_n)$ .

**Application 40** Soient  $n \in \mathbb{N}$ ,  $\mathbb{R}_n[X] = \{P \in \mathbb{R}[X] \mid \deg P \leq n\}$  et  $a \in \mathbb{R}$ .  $\forall k \in [0; n]$ , on pose

$$\varphi_k : \mathbb{R}_n[X] \rightarrow \mathbb{R}, P \mapsto P^{(k)}(a)$$

$(\varphi_k)_{k \in [0; n]}$  est une base de  $(\mathbb{R}_n[X])^*$  et  $(\frac{(X-a)^j}{j!})_{j \in [0; n]}$  est la base antéduale de  $(\varphi_k)_{k \in [0; n]}$ . Tout polynôme  $P$  de  $\mathbb{R}_n[X]$  s'écrit  $P = \sum_{i=1}^n \varphi_i(P) P_i$ , soit

$$P = \sum_{i=1}^n P^{(i)}(a) \frac{(X-a)^i}{i!}$$

ce qui est exactement la formule de Taylor. [MAD] p.173

## 4 Applications

### 4.1 Récurrence sur la dimension

**Définition 41** Définition du déterminant par récurrence sur la dimension

Soit  $A = (a_{ij}) \in \mathcal{M}_n(K)$ . On définit, par récurrence, une application  $\det : \mathcal{M}_n(K) \rightarrow K$  de la manière suivante :

- Si  $n = 1$ , (i.e.)  $A = (a)$ , on pose  $\det(A) = a$  ;
- Si  $n > 1$ , notons  $A_{ij}$  la matrice obtenue en supprimant la  $i^{\text{ème}}$  ligne et la  $j^{\text{ème}}$  colonne, on pose alors (puisque  $A_{ij} \in \mathcal{M}_{n-1}(K)$ ) :

$$\det(A) = a_{11} \det(A_{11}) + \dots + (-1)^{k+1} a_{1k} \det(A_{1k}) \\ + (-1)^{n+1} a_{1n} \det(A_{1n})$$

Le scalaire  $\det(A)$  est dit déterminant de  $A$  et on note

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} := \det \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

### [GRI] p.103-104

**Définition 42** Une base  $B$  de  $E$  est dite  $q$ -orthogonale si pour tout couple d'éléments distincts  $(e, e')$  de  $B$ , on a  $\varphi(e, e') = 0$ . [GRI] p.304

**Théorème 43** Si  $E$  est de dimension finie, il existe une base  $q$ -orthogonale de  $E$ . [GRI] p.305

**Théorème 44** Critère de Sylvester :

Soit  $M = (a_{i,j})_{1 \leq i, j \leq n} \in \mathcal{M}_n(\mathbb{R})$  une matrice symétrique. Alors

$M$  est définie positive si et seulement si  $\forall k \in \{1, \dots, n\}$ ,  $\det M_k > 0$ . [GOUal] p.243-244

**Application 45**  $A = (\frac{1}{1+|i-j|})_{1 \leq i, j \leq n}$  est symétrique définie positive. [GOUal] p.245

**Théorème 46** Soit  $k = \mathbb{F}_q$  un corps fini de caractéristique différente de 2, et  $E$  un  $k$ -espace vectoriel de dimension  $n$ .

Soit  $\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$ . Il y a deux classes d'équivalences de formes quadratiques non dégénérées sur  $E$ , de matrices

$$Q_1 = I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \text{ et} \\ Q_2 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & \alpha \end{pmatrix}$$

[PER] p.130

## 4.2 Calcul différentiel

**Théorème 47** ♠ Lemme de Morse ♠

Soit  $f : U \rightarrow \mathbb{R}$  une fonction de classe  $C^1$  sur un ouvert  $U$  de  $\mathbb{R}^n$  contenant l'origine. On suppose que  $Df(0) = 0$  et que  $D^2f(0)$  est non dégénérée, de signature  $(p, n - p)$ .

Alors il existe un difféomorphisme  $x \mapsto u := \varphi(x)$  entre deux voisinages de l'origine dans  $\mathbb{R}^n$ , de classe  $C^1$ , tel que

$$\varphi(0) = 0 \text{ et } f(x) - f(0) = u_1^2 + \dots + u_p^2 - u_{p+1}^2 - \dots - u_n^2$$

[ROU] p.354, p.210

**Théorème 48** ♠ Théorème des extrema liés ♠

Soit  $S = \{x \in U \mid g(x) = 0\}$ , où  $g : U \rightarrow \mathbb{R}^m$  est de classe  $C^1$ . On suppose que, pour tout  $x \in W$ ,  $Dg(x)$  est surjective. Soit aussi  $f : U \rightarrow \mathbb{R}$  une fonction de classe  $C^1$ .

Si  $p$  est un point critique de  $f|_S$ , alors il existe une forme linéaire  $\lambda : \mathbb{R}^m \rightarrow \mathbb{R}$  telle que

$$Df(p) = \lambda \circ Dg(p)$$

Autrement dit, pour tout  $v \in \mathbb{R}^n$ , nous avons  $Df(p)(v) = \lambda(Dg(p)(v))$ , ou encore, en écrivant  $\lambda(x) = \sum_{i=1}^m \lambda_i x_i$  : il existe  $\lambda_1, \dots, \lambda_m \in \mathbb{R}$  (dits des multiplicateurs de Lagrange) tels que, pour tout  $v \in \mathbb{R}^n$ ,

$$Df(p)(v) = \sum_{i=1}^m \lambda_i Dg_i(p)(v)$$

[BER] p.191 → 195

**Application 49** Grâce au théorème des extrema liés, on peut démontrer de façon amusante le théorème spectral :

Soit  $(E, \langle \cdot, \cdot \rangle)$  un espace euclidien,  $u \in \mathcal{L}(E)$  symétrique. Alors il existe une base orthonormée de  $E$  formée de vecteurs propres de  $u$ .

## 4.3 Systèmes d'équations différentielles linéaires [DTZ] p.522 → 527, [GOUan] p.358

**Théorème 50** Soit  $A : I \rightarrow \mathcal{M}_n(\mathbb{R})$  une fonction continue. L'ensemble  $\mathcal{S}_H$  des solutions maximales de l'équation différentielle linéaire homogène

$$y' = A(t)y \quad (H)$$

est un s.e.v. de dimension  $n$  du  $\mathbb{R}$ -e.v.  $C^1(I, \mathbb{R}^n)$ .

**Corollaire 51** Soient  $A : I \rightarrow \mathcal{M}_n(\mathbb{R})$  et  $B : I \rightarrow \mathbb{R}^n$  des fonctions continues. L'ensemble des solutions de l'équation différentielle linéaire

$$y' = A(t)y + B(t) \quad (\mathcal{L}_1)$$

est un espace affine de dimension  $n$ .

## 4.4 Extensions de corps [PER] p.65-66

**Définition 52** Une extension de corps est la donnée d'un morphisme injectif de corps  $i : K \rightarrow L$ , où  $K$  et  $L$  sont des corps. Notation :  $K \subset L$ . [ML3al] p.713

**Exemple 53**  $\mathbb{Q} \subset \mathbb{R}$  et  $\mathbb{R} \subset \mathbb{C}$ .

**Remarque 54** Si  $K$  est un sous-corps de  $L$ , alors  $L$  est un  $K$ -espace vectoriel.

**Définition 55** Si  $\dim_K L$  est finie, on définit le dégré de l'extension  $L$  sur  $K$  par  $[L : K] = \dim_K L$ .

**Remarque 56** Si  $K$  et  $L$  sont des corps finis, on a  $|L| = |K|^{[L:K]}$ .

**Théorème 57** Théorème de la base télescopique Soient  $K \subset L \subset M$  des corps,  $(e_i)_{i \in I}$  une base de  $L$  sur  $K$  et  $(f_j)_{j \in J}$  une base de  $M$  sur  $L$ . Alors la famille  $(e_i f_j)_{(i,j) \in I \times J}$  est une base de  $M$  sur  $K$ .

**Corollaire 58** Multiplicativité des degrés Dans la situation du théorème précédent, si les degrés sont finis, on a

$$[M : K] = [M : L][L : K]$$

## 4.5 Représentations linéaires de groupes [PEY] p.194 → 205

**Définition 59** Soit  $V$  un  $\mathbb{C}$ -espace vectoriel de dimension finie  $n$ . Une représentation linéaire d'un groupe  $G$  dans  $V$  est la donnée d'un morphisme  $\rho : G \rightarrow \text{GL}(V)$ . Ceci correspond à la donnée d'une action linéaire du groupe  $G$  sur  $V$  :

$$G \times V \rightarrow V \\ (g, v) \mapsto g.v = \rho(g)(v)$$

**Exemple 60** La représentation régulière à gauche est la représentation de  $G$  sur l'espace vectoriel  $\mathbb{C}[G]$  (espace vectoriel de dimension  $|G|$  sur  $\mathbb{C}$  dont la base est indexée par  $G$  et de la forme  $\{e_g\}_{g \in G}$ ) définie par le morphisme

$$\forall g \in G, \quad \rho(g) : \begin{cases} \mathbb{C}[G] & \rightarrow \mathbb{C}[G] \\ e_h & \mapsto e_{gh} \end{cases}$$

**Définition 61** • Soient  $\rho$  et  $\rho'$  deux représentations d'un même groupe  $G$  respectivement sur deux  $\mathbb{C}$ -espace vectoriel  $V$  et  $V'$ . Un opérateur d'entrelacement est une application linéaire  $\tau : V \rightarrow V'$  tel que pour tout  $g \in G$ ,  $\tau \circ \rho(g) = \rho'(g) \circ \tau$

$$\begin{array}{ccc} V & \xrightarrow{\tau} & V' \\ \rho(g) \downarrow & & \downarrow \rho'(g) \\ V & \xrightarrow{\tau} & V' \end{array}$$

- On note  $\text{Hom}_G(V, V')$  l'ensemble des opérateurs d'entrelacements.
- Deux représentations  $\rho$  et  $\rho'$  d'un même groupe  $G$  respectivement sur deux  $\mathbb{C}$ -espace vectoriel  $V$  et  $V'$  sont dites isomorphes (ou  $G$ -isomorphes) si  $\tau$  est bijective.

**Définition 62** (i) Si une représentation  $\rho$  de  $G$  sur  $V$  admet un sous-espace vectoriel  $W \subset V$  stable pour tous les  $\rho(g) \in \text{GL}(V)$ , elle induit une représentation  $\rho_W$  sur  $W$  appelée sous-représentation.  
(ii) Une représentation sur un espace  $V$  est dite irréductible si elle admet exactement deux sous-représentations :  $\{0\}$  et  $V$  tout entier.

**Théorème 63** Théorème de Maschke  
Toute représentation peut s'écrire comme somme de représentations irréductibles.

**Proposition 64** Lemme de Schur :

Soient  $\rho$  et  $\rho'$  deux représentations irréductibles d'un groupe  $G$  respectivement sur deux  $\mathbb{C}$ -espace vectoriel  $V$  et  $V'$  et  $f \in \mathcal{L}(V, V')$  un opérateur d'entrelacement. Alors

(i) si  $\rho$  et  $\rho'$  ne sont pas isomorphes,  $f = 0$ .

(ii) Si  $f \neq 0$ , alors  $f$  est un isomorphisme.

Si on suppose  $V = V'$ , alors  $f$  est une homothétie.

**Corollaire 65** On considère toujours deux représentations irréductibles d'un groupe  $G$  sur  $V$  et  $V'$ . On a donc

$$\dim(\text{Hom}_G(V, V')) = \begin{cases} 1 & \text{si } V \text{ et } V' \text{ sont} \\ & \text{isomorphes} \\ 0 & \text{sinon} \end{cases}$$

### Illustrations

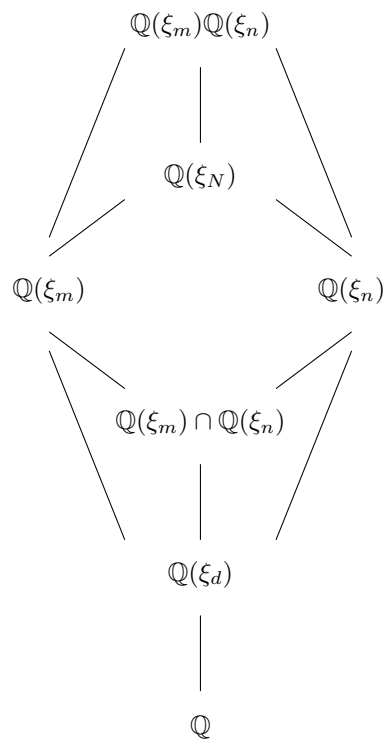


Figure 1

## Questions

### Exercice : Théorème de la base télescopique

Soient  $K \subset L \subset M$  des corps,  $(e_i)_{i \in I}$  une base de  $L$  sur  $K$  et  $(f_j)_{j \in J}$  une base de  $M$  sur  $L$ .  
Montrer que la famille  $(e_i f_j)_{(i,j) \in I \times J}$  est une base de  $M$  sur  $K$ .

*Solution* : Classiquement, nous allons montrer que la famille  $(e_i f_j)_{(i,j) \in I \times J}$  est libre et génératrice.

Famille libre : On suppose qu'il existe une famille  $(\lambda_{ij})_{(i,j) \in I \times J}$  d'éléments de  $K$  telle que

$$\sum_{(i,j) \in I \times J} \lambda_{ij} e_i f_j = 0$$

Par suite,

$$0 = \sum_{(i,j) \in I \times J} \lambda_{ij} e_i f_j = \sum_{j \in J} f_j \underbrace{\left( \sum_{i \in I} \lambda_{ij} e_i \right)}_{\in L}$$

Or, comme  $(f_j)_{j \in J}$  une base de  $M$  sur  $L$ , on en déduit que

$$\forall j \in J, \sum_{i \in I} \lambda_{ij} e_i = 0$$

et puis comme  $(e_i)_{i \in I}$  une base de  $L$  sur  $K$ , on en déduit que

$$\forall j \in J, \forall i \in I \quad \lambda_{ij} = 0$$

Famille génératrice : Soit  $x \in M$ , on peut écrire, puisque  $(f_j)_{j \in J}$  une base de  $M$  sur  $L$ ,

$$x = \sum_{j \in J} \mu_j f_j \quad \text{avec } \mu_j \in L$$

Puis, on peut décomposer chaque  $\mu_j$  dans  $(e_i)_{i \in I}$  qui est une base de  $L$  sur  $K$  (i.e.)

$$\forall j \in J, \mu_j = \sum_{i \in I} \lambda_{ij} e_i \quad \text{avec } \lambda_{ij} \in K$$

Finalement,

$$x = \sum_{j \in J} \mu_j f_j = \sum_{j \in J} \mu_j \left( \sum_{i \in I} \lambda_{ij} e_i \right) = \sum_{(i,j) \in I \times J} \lambda_{ij} e_i f_j$$

avec  $\lambda_{ij} \in K$ . D'où le résultat.

**Exercice** : Soit  $p$  un nombre premier et  $n \in \mathbb{N}^*$ . On note  $q = p^n$ .

- 1) Montrer que le corps fini  $\mathbb{F}_{q^n}$  admet un unique sous-corps  $\mathbb{F}_q$  à  $q$  éléments et que  $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ .
- 2) En déduire que tout corps intermédiaire  $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$  est un corps  $\mathbb{F}_{q^d}$  à  $q^d$  éléments où  $d$  est un diviseur de  $n$  et que, pour chaque diviseur  $d$  de  $n$ , il existe un unique corps intermédiaire de cardinal  $q^d$ .

*Solution* : 1) Unicité : S'il existe un sous-corps  $K$  de  $\mathbb{F}_{q^n}$  ayant  $q$  éléments, alors le groupe multiplicatif  $K^*$  (qui a  $q - 1$  éléments) vérifie

$$\forall x \in K^*, x^{q-1} = x \quad \Rightarrow_{0^{q-1}=0} \quad \forall x \in K, x^{q-1} = x$$

Par suite, il en résulte que tout  $x \in K$  est une racine du polynôme  $X^q - X$ . Ce polynôme étant de degré  $q$ ,  $K$  est le corps de décomposition de  $X^q - X$  sur  $\mathbb{F}_p$ . Ainsi, si  $K$  existe, alors  $K$  est unique (par unicité



du corps de décomposition).

Existence : On sait  $\mathbb{F}_{q^n}$  est le corps de décomposition de  $X^{q^n} - X$  sur  $\mathbb{F}_p$  et  $X^q - X \mid X^{q^n} - X$ .

**Rappel** : Pour  $a, b \in \mathbb{N}^*$ , on a  $X^a - 1 \mid X^{ab} - 1$ .

*Ch'tite démonstration* :

$$X^{ab} - 1 = (X^a)^b - 1 = (X^a - 1)(1 + (X^a)^2 + \dots + (X^a)^{b-1})$$

D'où le résultat. □

Donc  $\mathbb{F}_{q^n}$  contient un corps de décomposition de  $X^q - X$  et un tel corps contient  $q$  éléments. D'où l'existence.

Calcul du degré : Soit  $m = [\mathbb{F}_{q^n} : \mathbb{F}_q]$ . Ce qui se traduit par le fait que  $\mathbb{F}_{q^n}$  est un  $\mathbb{F}_q$ -e.v. de dimension  $m$  et donc  $|\mathbb{F}_{q^n}| = |\mathbb{F}_q|^m$ . Par suite,  $q^n = q^m$ , d'où  $m = n$ .

2) Soit  $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$  et soit  $d = [K : \mathbb{F}_q]$ . Alors  $|K| = |\mathbb{F}_q|^d = q^d$  et par multiplicativité des degrés, on a

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : K][K : \mathbb{F}_q]$$

Donc  $d \mid n$

Réciproquement, soit  $d$  un diviseur de  $n$ . Posons  $r = q^d$ . Alors  $\mathbb{F}_{q^n} = \mathbb{F}_{r^m}$  où  $m = \frac{n}{d}$  et, d'après ce qui précède, il existe un unique sous-corps  $\mathbb{F}_r$  dans  $\mathbb{F}_{r^m}$ .

**Exercice** : Soient  $m$  et  $n$  des entiers naturels non nuls. On pose  $N = \text{ppcm}(m, n)$  et  $d = \text{pgcd}(m, n)$ . Pour tout  $t \in \mathbb{N}^*$ , on désigne par  $\xi_t$  une racine primitive  $t$ -ième de l'unité. Montrer que

(i)  $\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_N)$

(ii)  $\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_d)$

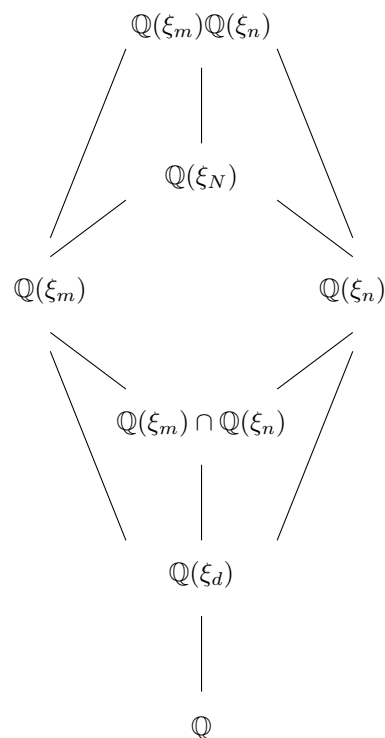
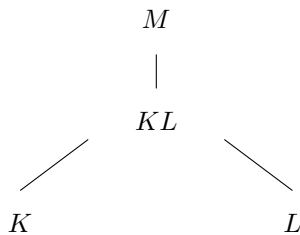
*Solution* :

**Rappel 1** : Soient  $K$  et  $L$  deux sous-corps d'un corps  $M$ . Par définition  $KL$  est le plus petit sous corps de  $M$  contenant  $K$  et  $L$ . L'opération

$$(K, L) \rightarrow KL$$

$$(k, l) \mapsto kl$$

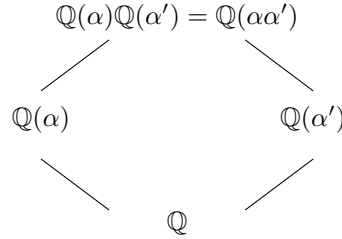
est commutative et associative et si  $K \subseteq L$ , alors  $KL = L$



**Rappel 2 :** Soit  $\alpha$  (resp.  $\alpha'$ ) une racine  $p$ -ième (resp.  $q$ -ième) de l'unité. Si  $\text{pgcd}(p, q) = 1$  alors  $\alpha\alpha'$  est une racine  $pq$ -ième de l'unité, et donc on a

$$\mathbb{Q}(\alpha)\mathbb{Q}(\alpha') = \mathbb{Q}(\alpha\alpha')$$

On peut étendre ce résultat par récurrence à plus de deux racines de l'unité.



*Ch'tite démonstration :* Montrons que si  $\alpha$  et  $\alpha'$  sont respectivement des racines  $p$ -ième et  $q$ -ième de l'unité avec  $\text{pgcd}(p, q) = 1$  alors  $\alpha\alpha'$  est une racine  $pq$ -ième de l'unité.

Cela provient du résultat plus général suivant (et à connaître!) :

«Soient  $a$  et  $b$  des éléments d'ordre  $p$  et  $q$  d'un groupe  $G$ . On suppose que  $a$  et  $b$  commutent et que  $p$  et  $q$  sont premiers entre eux, alors  $ab$  est d'ordre  $pq$ .»

Notons  $n$  l'ordre de  $ab$ . Comme  $a$  et  $b$  commutent, on a  $(ab)^{pq} = a^{pq}b^{pq} = 1$ , donc  $n$  (l'ordre de  $ab$ ) divise  $pq$ .

Inversement, si  $(ab)^n = 1 = a^n b^n$ , on a

$$a^{nq} \underbrace{b^{nq}}_{=1} = 1 \Rightarrow a^{nq} = 1$$

Donc l'ordre de  $a$  (qui est  $p$ ) divise  $nq$  mais comme  $p$  et  $q$  sont premiers entre eux, alors  $p \mid n$ . On applique le même raisonnement à  $b$  et on en déduit que  $q \mid n$ . Par conséquent,  $pq \mid n$ . D'où le résultat. □

Maintenant les rappels faits, revenons à notre exercice.

(i) Ecrivons  $n$ ,  $m$  et  $N$  en produit de facteurs premiers distincts :

$$m = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \quad n = p_1^{\beta_1} \dots p_k^{\beta_k}, \quad N = p_1^{\gamma_1} \dots p_k^{\gamma_k}$$

où  $\alpha_j, \beta_j \geq 0$ ,  $\gamma_j = \max(\alpha_j, \beta_j) \neq 0$  pour tout  $j \in \{1, \dots, k\}$ .

D'une part, d'après le Rappel 2, on a

$$\mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_{p_1^{\alpha_1}}) \dots \mathbb{Q}(\xi_{p_k^{\alpha_k}}) \quad (\dagger)$$

$$\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{p_1^{\beta_1}}) \dots \mathbb{Q}(\xi_{p_k^{\beta_k}}) \quad (\dagger\dagger)$$

D'autre part, pour  $a, b \in \mathbb{N}^*$ , on a  $\mathbb{Q}(\xi_a) \subseteq \mathbb{Q}(\xi_{ab})$ . En effet,  $\xi_a$  est une racine de  $X^{ab} - 1 = (X^a)^b - 1$  et  $\mathbb{Q}(\xi_{ab})$  est le corps de décomposition du polynôme  $X^{ab} - 1$ . Avec le Rappel 1, on a donc, pour tout  $j \in \{1, \dots, k\}$

$$\mathbb{Q}(\xi_{p_j^{\alpha_j}})\mathbb{Q}(\xi_{p_j^{\beta_j}}) = \mathbb{Q}(\xi_{p_j^{\gamma_j}})$$

Grâce à  $(\dagger)$  et  $(\dagger\dagger)$ , on a donc

$$\begin{aligned}
 \mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n) &= \mathbb{Q}(\xi_{p_1^{\alpha_1}}) \dots \mathbb{Q}(\xi_{p_k^{\alpha_k}}) \mathbb{Q}(\xi_{p_1^{\beta_1}}) \dots \mathbb{Q}(\xi_{p_k^{\beta_k}}) \\
 &= [\mathbb{Q}(\xi_{p_1^{\alpha_1}}) \dots \mathbb{Q}(\xi_{p_k^{\alpha_k}})] [\mathbb{Q}(\xi_{p_1^{\beta_1}}) \dots \mathbb{Q}(\xi_{p_k^{\beta_k}})] \\
 &= \mathbb{Q}(\xi_{p_1^{\alpha_1}})\mathbb{Q}(\xi_{p_1^{\beta_1}}) \dots \mathbb{Q}(\xi_{p_k^{\alpha_k}})\mathbb{Q}(\xi_{p_k^{\beta_k}}) \\
 &= \mathbb{Q}(\xi_{p_1^{\gamma_1}}) \dots \mathbb{Q}(\xi_{p_k^{\gamma_k}}) \\
 &= \mathbb{Q}(\xi_{p_1^{\gamma_1} \dots p_k^{\gamma_k}}) = \mathbb{Q}(\xi_N)
 \end{aligned}$$

(ii) Par commodité, posons  $k = \mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n)$ . Par définition,  $d \mid n$  et  $d \mid m$ , on a donc  $\mathbb{Q}(\xi_d) \subseteq k$ . Par ailleurs, on a

$$\underbrace{[\mathbb{Q}(\xi_m) : \mathbb{Q}]}_{\varphi(m)} = [\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_d)] \underbrace{[\mathbb{Q}(\xi_d) : \mathbb{Q}]}_{\varphi(d)}$$

d'où

$$[\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_d)] = \frac{\varphi(m)}{\varphi(d)}$$

Puis, par la question précédente, on a

$$\begin{aligned} [\mathbb{Q}(\xi_n)\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_m)] &= [\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_m)] = \frac{\varphi(N)}{\varphi(m)} \\ [\mathbb{Q}(\xi_n)\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_n)] &= [\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_n)] = \frac{\varphi(N)}{\varphi(n)} \end{aligned}$$

### Rappel 3 :

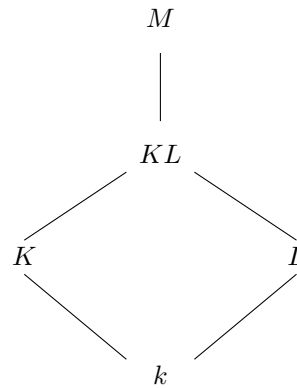
Soit  $k \subset M$  une extension,  $K$  et  $L$  deux corps intermédiaires,  $KL$  le sous-corps de  $M$  engendré par  $K$  et  $L$ . Alors on a

$$[KL : L] \leq [K : k]$$

*Ch'tite démonstration :* Tout élément de  $KL$  s'écrit sous la forme

$$x = \sum u_i v_i \quad \text{avec } u_i \in K, v_i \in L$$

Ainsi, si  $(x_1, \dots, x_n)$  est une base de  $K$  sur  $k$ , alors  $(x_1, \dots, x_n)$  engendrent  $KL$  sur  $L$ . □



Par le Rappel 3, on en déduit que

$$[\mathbb{Q}(\xi_n)\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_n)] \leq [\mathbb{Q}(\xi_m) : k]$$

Par suite,

$$[\mathbb{Q}(\xi_n)\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_n)] = \frac{\varphi(N)}{\varphi(n)} \leq [\mathbb{Q}(\xi_m) : k] \leq [\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_d)] \leq \frac{\varphi(m)}{\varphi(d)}$$

Cependant, comme  $mn = Nd$ , on a donc par multiplicativité de la fonction  $\varphi$ ,

$$\varphi(m)\varphi(n) = \varphi(N)\varphi(d)$$

Ainsi, on obtient

$$\frac{\varphi(N)}{\varphi(n)} \leq [\mathbb{Q}(\xi_m) : k] \leq [\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_d)] \leq \frac{\varphi(m)}{\varphi(d)} \xrightarrow{\varphi(m)\varphi(n) = \varphi(N)\varphi(d)} [\mathbb{Q}(\xi_m) : k] = [\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_d)]$$

Et comme  $\mathbb{Q}(\xi_d) \subseteq k \subseteq \mathbb{Q}(\xi_m)$ , on a bien  $\mathbb{Q}(\xi_d) = k$ . D'où le résultat.

